コンピュータセキュリティ　14−31
（2001. 7. 25）

不正侵入者を外部ネットワークに設置したおとりサーバへ誘導するセキュリティシステムの検討

宮川 明子，稲田 徹，後沢 忍

三菱電機株式会社 情報技術総合研究所
〒247 - 8501 神奈川県鎌倉市大船５－１－１
m-akiko@isl.melco.co.jp，inaina@isl.melco.co.jp，ussy@isl.melco.co.jp

あらまし
今日、ネットワーク利用者にとってセキュリティ対策の重要性が認められるようになり、市場でも様々なセキュリティ対策製品・サービスが展開されている。その中で、不正侵入者を攻撃対象に見せかけた仮想的なマシンにアクセスさせ、その行動を監視し、情報収集を行うおとりツールが、不正侵入検知の新たなアプローチとして登場してきた。本稿では、おとりシステムを利用した不正侵入対処サービスを想定し、保護対象サーバの外部におとりサーバを設け、侵入検知時に不正侵入者をおとりサーバへ誘導するシステムとその方式について提案する。

キーワード　ネットワークセキュリティ、侵入検知、おとりサーバ

A Security System Redirecting Attackers to Decoy Servers on Outside Networks

Akiko Miyagawa, Toru Inada, Shinobu Ushirozawa

Information Technology R&D Center, Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura, Kanagawa 247-8501, Japan
m-akiko@isl.melco.co.jp，inaina@isl.melco.co.jp，ussy@isl.melco.co.jp

Abstract
Recently, it is well known that network security action is very important for computer network users. Many security products and services are provided for such a market. As a new approach to counter attackers, decoy tools which mislead attackers into a virtual machine and log their behavior.
In this paper, we propose a security system and method using decoy servers on the outside network for security services. In the system, packets of attackers are redirected to a decoy server when an intrusion is detected.

key words　Network Security, Intrusion Detection System, Decoy server

1．はじめに

ネットワークを利用して誰もが様々な情報にアクセスできるようになった今日、ネットワーク上の脅威は確実に増加しており、マスコミでも数々のネット犯罪が取上げられるようになった。このような背景から、情報資源に対するセキュリティ対策の重要性が認識されつつあり、市場にも様々なセキュリティ対策製品やサービスが展開されている。

セキュリティ対策のために使用される製品には、不要なパケットを遮断し、組織内ネットワークの防御壁の役割を果たすファイアウォール、ウィルスの感染予防・駆除を行うウィルス対策ソフト、不正アクセスを防ぐ各種認証サーバやIDS(Intrusion Detection System)、安全な通信経路を確保するVPN（Virtual Private Network）装置などがある。また、不正侵入検知の新たなアプローチとして、不正侵入者を攻撃対象に見せかけた仮想的なマシンにアクセスさせ、その行動を監視し、情報収集を行うおとりツールも登場してきた。

おとりツールの事例として、CyberCop String(Network Associates 社)[1]、ManTrap(Recourse 社）[2]といった製品や、実験プロジェクトHoneynetProject[3]が知られている。しかし、これらはあらかじめセキュリティの低いサーバを公開しておくことで、不正侵入者をおびきよせることを前提としたもので、不正侵入者がおとりツールに接触しなければ、効果が得られない。

そこで、本稿では、不正侵入者を意図的におとりサーバへ誘導する方式について提案する。2章で本研究の目的、3章で提案システムの内容について述べる。最後に、4章で本システムを実現するための今後の検討課題を示し、まとめとする。

2．本研究の目的

おとり技術を用いたシステムの要件として、

（1）不正侵入者に気付かれない。

（2）攻撃対象となったサーバを保護する。

（3）正規ユーザからのアクセスには、通常サービスを提供する。

が挙げられる。また、おとり技術の実現方法としては、主に

- 同一サーバ内におとり領域を設ける
- 保護対象サーバとは別に、おとり用の擬似サーバを設ける

がある。このうち、前者は攻撃対象となったサーバ自身におとり機能が必要であるため、保護したいサーバの数だけインストールが必要となる。また、後者に比べ、攻撃を受けた場合のおとり機能への影響が大きく、要件（2）への安全性が低い。一方で、後者は、おとりサーバと保護対象サーバの状態を同期させる仕組みが複雑となるが、おとり機能を独立させるため、安全性は高い。

将来的に、おとりシステムを利用した不正侵入対処サービスを想定した場合、後者の方が有効な手段になると考えられる。そこで、我々は保護対象サーバの外部におとりサーバを設ける後者の方法に注目した、おとり誘導方式について提案する。

3．おとり誘導システム

竹森ら[4][5]は、上記、両方の方法を想定したモデルを提案している。このうち我々が注目している後者の方法に関しては、公開サーバに侵入検知プロセス、通信中継プロセスを設け、ルータにセッション引継ぎ要求を通知する方式を取っている[4]。この方式によるセキュリティサービスの提供を考えた場合、顧客（サービス契約者）への導入において、公開サーバ、おとりサーバ、ルータのそれぞれにおとりサービス専用のプログラムを適用する必要がある。

我々は、公開サーバ、ルータ等の既存の機器に手を加えることなく、最小限の導入手続きでサービスを実現するというアプローチを取った。これまでに、我々は既存のネットワークに影響を与えずに VPN 機能をアドオンするための技術（エンカプセルリピータ[6]）の研究を行ってきており、社内に、不正侵入を検知し自動的に駆除するシステムの技術[7]も保有している。これらの技術をベースに、不正侵入者からのパケットをセキュリティコンポーネントによりカプセル化し、外部に設置されたおとりサーバへ転送する方式を提案する。

3．1システムの構成

図1に、提案するシステム構成図を示す。

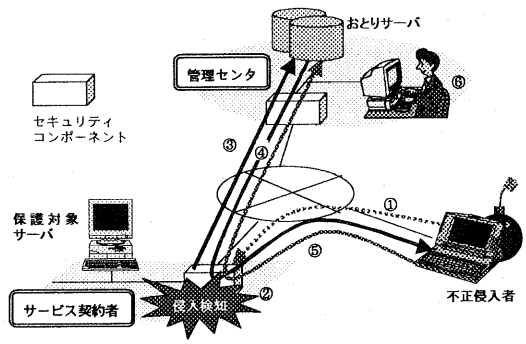

図1：システム構成図

本システムは、セキュリティサービスを提供する管理センタと、セキュリティサービスを契約している顧客のネットワークから構成される。管理センタには、管理装置、セキュリティコンポーネント、おとりサーバが設置されており、セキュリティコンポーネントは、サービス契約者のネットワークにも設置する。

また、おとりサーバには、サービス契約者の保護対象サーバと同じ IP アドレス空間、OS の環境を模擬しておく。

本稿では、セキュリティコンポーネントを不正侵入検知機能および通信パケットエンカプセル・デカプセル機能を持つセキュリティ装置、もしくはモジュールと定義する。セキュリティコンポーネントには、あらかじめ不正侵入と判断する基準（シグニチャ）を登録しておき、不正侵入を検知した場合に、所定の手順にしたがって、おとりサーバへの転送処理を開始する。

３．２誘導操作の流れ

本システムは、以下の手順で動作する。

① 不正侵入者がサービス契約者のネットワークに侵入しようとする。

② セキュリティコンポーネントで不正侵入を検知する。

③ セキュリティコンポーネントは不正侵入者の通信パケットをエンカプセル処理し、管理センタに転送する。転送されたパケットは、管理センタのセキュリティコンポーネントによりデカプセル処理され、おとりサーバに届けられる。

④ おとりサーバからの応答パケットは管理センタのセキュリティコンポーネントでエンカプセル処理後、サービス契約者のセキュリティコンポーネントに転送され、再びデカプセル処理後、不正侵入者に送信される。

⑤ 以降、不正侵入者はサービス提供者の保護対象サーバに侵入していると思い込むが、実際は、管理センタのおとりサーバとやりとりを行うことになる。

⑥ 管理センタにてログの収集・解析を行い、不正侵入者を追跡・特定し、対処する。

３．３ セキュリティコンポーネント

次にセキュリティコンポーネントの機能に着目した処理手順を述べる。

図２は、セキュリティコンポーネントの機能ブロック図である。セキュリティコンポーネントは、大きく分類すると、パケット送受信部、パケット識別部、不正侵入検知部、パケットエンカプセル・デカプセル部から構成される。

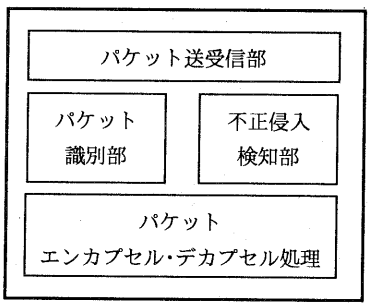

図２：セキュリティコンポーネントの機能ブロック

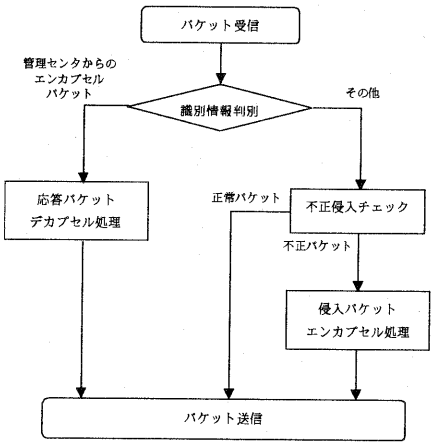

図３：サービス契約者のセキュリティコンポーネントの処理フロー

パケット送受信部は、通常のネットワーク機器が保持する機能を実現する。受信部では、外部からのパケットを受信するとパケット識別部に渡す。送信部では、エンカプセル部から渡された

パケットデータを外部に送信したり、正常パケットをそのまま中継する。パケット識別部では、通常パケットかエンカプセル処理されたパケットかを識別する。通常パケットの場合は、不正侵入検知部に渡す。エンカプセルパケットの場合は、デカプセル部に渡す。エンカプセル部は、転送すべきデータを隠蔽するためのカプセル処理（ヘッダ追加）を施し、パケット送信部に渡す。デカプセル部は、パケット識別部でエンカプセルパケットと判断されたパケットをデカプセル処理（ヘッダ除去）する。サービス契約者のセキュリティコンポーネントにおける以上の処理フローを図3に示す。

3．4パケット転送

図4にサービス契約者と管理センタのセキュリティコンポーネントの間でやりとりされるパケットの形態を示す。転送パケットは、オリジナルパケットをカプセル化するために追加され、通常のIPプロトコル処理が行われる**新IPヘッダ**、データの身元確認と改竄検証を行うための**認証情報**（署名）、エンカプセルデータであることや、顧客や転送フェーズを識別するための**識別情報**、転送データとしての**オリジナルパケット**（IPヘッダを含む）から構成される。セキュリティコンポーネントのエンカプセル処理、デカプセル処理によって、新IPヘッダ、認証情報、識別情報が追加、削除される。識別情報は、管理センタで保持しているサービス契約者の顧客DBとも照合される。

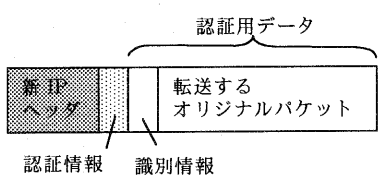

図4：転送パケットの形態

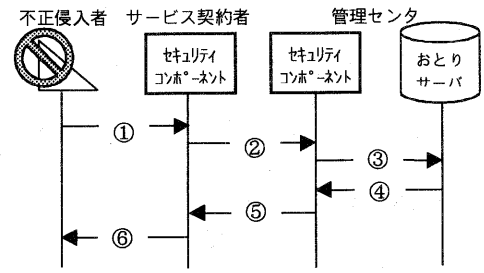

図5：パケットの転送フェーズ

表1：転送パケットの内容

転送フェーズ		新IPヘッダ		オリジナルパケット		
		送信元	宛先	送信元	宛先	データ部
①	A → CS	−	−	A	CT/CS	Aの情報
②	CS → MS	CS	MS	A	CT/CS	Aの情報
③	MS → D	−	−	A	CT/CS（=D）	Aの情報
④	D → MS	−	−	D	A	Dの情報
⑤	MS → CS	MS	CS	D	A	Dの情報
⑥	CS → A	−	−	D	A	Dの情報

A:不正侵入者、CS:サービス契約者のセキュリティコンポーネント、CT:サービス契約者の端末、MS:管理センタのセキュリティコンポーネント、D:管理センタのおとりサーバ

この転送パケットは、Well-Known 以外の特定ポートを利用した独自プロトコルを想定している。なお、エンカプセル処理において、オリジナルパケットを暗号化することも検討している。

また、転送パケットは、図5に示すような転送フェーズに従って、エンカプセル・デカプセル処理が施される。各フェーズにおけるパケットの内容を表1に示す。まず、不正侵入者（以下A）から攻撃対象に向けて侵入用のパケットが送信される（フェーズ①）。表1では送信元アドレスはAとしているが、なりすましによりこの限りではない。次に、サービス契約者のセキュリティコンポーネント（以下CS）がこの侵入用パケットを不正侵入と判断すると、CSでエンカプセル処理し、管理センタのセキュリティコンポーネント（以下、MS）に送る（フェーズ②）。管理センタでは、MSでそのパケットをデカプセル処理しAからの情報をおとりサーバ（以下、D）に送信する（フェーズ③）。Aへの応答パケットをDにて生成し、フェーズ①～③とは逆の手順によりAに返す（フェーズ④～⑥）。Aにとっては、自分がフェーズ①で送信した宛先（CSもしくはST）からの応答に見えるが、実際はDからの応答である。

4．まとめと今後の検討課題

本稿では、不正侵入対処システムの一方式として、攻撃対象とは独立した環境に設置したおとりサーバに不正侵入者のパケットを転送することにより、攻撃対象を守る方式を提案した。現状では、おとり誘導システムの方式について枠組みを提示したものであるため、今後、より具体的な検討が必要となる。以下に、今後の具体的検討項目を挙げる。

- TCP/IPプロトコルやアプリケーションに着目した転送タイミングと詳細なシーケンス
- パケット識別項目の定義
- パケットフラグメント時におけるリアセンブル処理方法
- パケットの認証処理、カプセル処理におけるスループット評価
- 大規模システムにおけるおとりサーバとセキュリティコンポーネントの管理方法と負荷分散
- ビジネスモデルとしてのサービスのあり方

【参考文献】

[1] Cyber Cop String,<http://www.nai.com>.

[2] ManTrap,<http://www.dit.co.jp/recourse/mantrap.html>.

[3] Honeynet Project,<http://project.honeynet.org/>.

[4] 竹森,田中,中尾,"不正侵入者に検知されない通信セッションのおとりサーバへの引継ぎ方式の検討",情報処理学会第61回全国大会論文集,4F-03,2000.

[5] 竹森,田中,清本,中尾," 不正侵入者に検知されることなくおとりのデータ領域へと誘導するおとりシステムの実装評価",情報処理学会研究報告 01-CSEC-12 pp.79-84,Feb 2001.

[6] 稲田,後沢,時庭他, "VPN構築技術の検討・リピータターキテクチャ", 情報処理学会第61回全国大会論文集,4G-02,2000.

[7] 大越,木下," 侵入検知に対する対策の自動解除", 情報処理学会第61回全国大会論文集, 4F-01,2000.